



Commonwealth Office of Technology

Monthly Cyber Security Tips

January 2009

Volume 4, Issue 1

Challenge or Secret Questions

From the Office of COT's Chief Information Security Officer

What are Challenge or Secret Questions?

Knowledge-based authentication or the use of "Challenge or Secret Questions" helps computer users access their accounts when they forget their password. The questions are often designed as simple, easy-to-remember "prompts" that only the authorized user should be able to answer. They are in effect a backup to your password.

While some systems allow users to create their own challenge or secret questions, most systems have pre-populated questions such as "What is your mother's maiden name? What is the name of your first pet or car? What is your favorite color?" While these systems are a great convenience for the end user (they are not likely to forget the responses) and are efficient from the administrator's perspective (low overhead), they are very weak from a security perspective.

What are the security concerns with using Challenge or Secret Questions?

There is a limited pool of secret questions that most Knowledge-Based Authentication systems use and many of the questions have a limited amount of potential responses, such as "What is your favorite color?" If someone researches you and discovers the answers for your questions, they could gain unauthorized access to your account.

The ability for someone to guess the response to a user's secret question has greatly increased due to the large volume of information available on the Internet. This was demonstrated during the recent presidential campaign, when one of the candidate's email accounts was hacked into. The attacker was able to do so by conducting a minimal amount of research about the candidate using information found on the Internet to answer the secret questions and get the password for the email account.

Users need to be aware that there is a tremendous amount of information available about them, not only through Internet search engines, but also social networking profiles and other sources.

What can be done to make Challenge or Secret Questions more secure?

As with the design of a regular password, the responses to secret questions should be something that is hard to guess, but easy to remember. Users are encouraged to not provide the technically correct response to the question. Similar to developing a strong password, the response to a secret question is in effect a password and thus should have the same protections. The use of a combination of upper and lower case letters, special characters and numbers is recommended. There are many ways to obfuscate your response. The key is to develop a methodology that is easy for you to remember but difficult for someone else, even someone you know, to guess. Some examples are:

1. Begin and/or end each response with a number, capitalize a letter and use a special character. For example, the response to your mother's maiden name of "Smith" would be "44Smith!" OR Insert a number and special character in the middle of the word. In this example the response to your mother's maiden name of "Smith" would be "Smi44!th."
2. Provide answers that do not correspond to the question, thus making it difficult for an attacker to correctly guess. For example, a user may use the name of a city as the response for "mother's maiden name."
3. Use the question itself to create an easy-to-remember passphrase. By combining the main part of the question with one of your favorite catchwords, you can create a passphrase they can remember. If the question is asking for your favorite sports team, you can combine "Sports Team" from the question and combine it with a phrase from your favorite show, such as "CSI." Their answer is, "Sports Team CSI."
4. Follow best practices for strong passwords when developing your responses, such as making it at least 8 characters long and using numbers, upper and lower case letters, and special characters. The answers can be different on different websites, even if the same secret question is used. Thus a hacker won't potentially have access to other accounts if one is compromised.
5. As with passwords, do not share the responses to your Challenge or Secret Questions, or your methodology for developing them, with anyone.

It is also advised to periodically search your name in an Internet search engine so you are aware of what information about you is freely accessible on the Internet.

For additional information on Challenge or Secret Questions, please visit:

US CERT www.us-cert.gov/cas/tips/ST04-002.html
US CERT www.us-cert.gov/cas/tips/ST05-012.html
OWASP www.owasp.org/index.php/Using_Secret_Questions

For more cyber security monthly tips go to:

www.msisac.org/awareness/news/
technology.ky.gov/security/CyberAwareness.htm

Brought to you by:

